

SEGURIDAD EMPRESARIAL

S E R V I C I O

SECURED

La Protección
que su Negocio
Necesita



nextiraOne
México

SECURED

La protección que su negocio necesita.

Las personas como las organizaciones siempre deben lidiar con el riesgo. Por lo cual buscamos la manera de asegurar nuestros bienes, seres queridos y todo aquello que consideramos de valor. Protegiendo en caso de que algo falle el futuro de nuestro patrimonio.

Esto aplica también a su negocio, donde **su infraestructura, su personal y su información corren riesgo** de ser transgredidos por un tercero no deseable, pudiendo caer en malas manos llegando incluso a ocasionar desperfectos que interrumpan o detengan la operación de su organización.

Diariamente **las instituciones encaran el riesgo como una parte de hacer negocios**. Un riesgo del negocio es la posibilidad de que algo indeseable suceda a la organización, sus clientes o una entidad de la cual el negocio dependa. Típicamente, la mayoría de los riesgos del negocio son cuantificado en términos económicos tales como pérdida de rentabilidad, pérdida de oportunidad o daño a la marca.

UNA ORGANIZACIÓN ES "SEGURA" CUANDO ENTIENDE LOS RIESGOS Y ES CAPAZ DE MANEJARLOS.

Las maneras en que las organizaciones pueden administrar éstos riesgos son:

- **Transfiriéndolos.** Una empresa puede transferir sus riesgos a terceros.
- **Mitigándolos.** Se puede reducir el riesgo disminuyendo la probabilidad de que el evento adverso ocurra al corregir las causas.
- **Evitándolos.** Una empresa puede escoger no comprometerse en actividades que creen cierto tipo de riesgos.
- **Aceptándolos.** Pueden escoger aceptar las consecuencias.

Para ayudar en la decisión de cómo administrar el riesgo de su empresa existen metodologías probadas mediante las cuales es posible **identificar y entender las vulnerabilidades de su institución** basadas en mejores prácticas reconocidas en el ámbito internacional facilitando la implementación de una seguridad empresarial y considerando barreras tanto físicas, lógicas como privadas para los usuarios, procesos y recursos.

La seguridad nunca es absoluta. No existe la "total seguridad". Las personas tanto como las organizaciones siempre enfrentan riesgos. Algunos de ellos pueden ser eliminados, otros reducidos y algunos aceptados. Pero siempre con el entendimiento de que cualquier seguridad puede ser quebrantada. **Una organización es "segura" cuando entiende los riesgos y es capaz de manejarlos** de manera que los costos usados para reducir los riesgos sean equiparables al valor de negocio esperado.

PRUEBAS DE CONCEPTO

PERMÍTANOS BAJO UN ESTRICTO
CÓDIGO DE ÉTICA DEMOSTRARLE LAS
TÉCNICAS REALES DE ATAQUE A LOS
COMPONENTES DE LA
INFRAESTRUCTURA DE SU RED.

¿Cómo aplicar los adecuados recursos de seguridad para administrar los riesgos del negocio?

Consultoría de seguridad

La respuesta mas confiable es contar con la consultoría de un socio de negocios que le ayude a identificar y administración las vulnerabilidades de seguridad de su organización basado en un código de ética profesional y fundamentado en metodologías usadas por organismos internacionales dedicados al aseguramiento de infraestructuras de TI.

¿Porqué elegir a NextiraOne como consultor de seguridad para su red empresarial?

Consultoría de Seguridad

NextiraOne México. Con el apoyo de los fabricantes líderes de equipos de redes y seguridad NextiraOne México cuenta con un grupo de expertos certificado en tecnologías, definición de procesos y metodologías basadas en estándares mundiales.

Más de 20 años en el mercado de telecomunicaciones en México. NextiraOne México es uno de los socios de tecnología reconocidos por los fabricantes por su experiencia en implementación de tecnologías emergentes en las redes empresariales.

Expertos en redes complejas. Apoyados en ese conocimiento sabemos que en los últimos años los ataques informáticos de las infraestructuras organizacionales utilizan ese medio para alcanzar sus objetivos, donde al incluirnos en su estrategia de seguridad atacamos el punto medular de la seguridad, auxiliándolo en el manejo de los riesgos.

Conocimiento del negocio. Comprendemos las necesidades de su negocio, las aplicaciones y la red que sustenta el funcionamiento de su organización, así como el entorno y regulaciones a las que aplica dependiendo del giro del mismo.

Servicios de Consultoría en Seguridad. Ponemos a sus ordenes nuestros servicios enfocados en apoyarlo en la administración e implantación de controles para la seguridad como: **Servicio de Valoración de Vulnerabilidades en la Red, Diseño de Sistemas de Administración de Seguridad de la Información, Diseño de Soluciones de Seguridad en Redes Complejas, Definición de Políticas de Seguridad Organizacionales, Elaboración de Planes de Concientización de Seguridad Organizacional y Seguridad de Infraestructura para Comunicaciones IP.**

www.NextiraOne.com.mx

SECURED SERVICES

Ayudando a las organizaciones a administrar el riesgo nos hemos enfocado en los factores primordiales para el buen desempeño de la operación de su negocio, apoyándoles con nuestro conocimiento de las redes enfocados a la seguridad.

Servicio de Valoración de Vulnerabilidades en la Red.*

Reconocimiento de los riesgos que su red empresarial y organización corren, brindándole herramientas para priorizar y comprender las áreas de oportunidad de su infraestructura.

- **Recolección de Información.**
- **Revisión de la Arquitectura de Seguridad de la Red.**
- **Sondeo de Vulnerabilidades.**
- **Análisis de Vulnerabilidades.**
- **Pruebas de Penetración.**
- **Documento de Resultados de Servicios de Valoración a nivel:**
 - Ejecutivo y
 - Técnico
- **Recomendaciones de Áreas de Oportunidad en Seguridad de su Infraestructura de Red.**

Diseño e Implantación de Sistemas de Administración de Seguridad de la Información.*

En base a las necesidades específicas de su compañía y en conjunto con usted desarrollaremos un plan para implementar las mejores prácticas de seguridad basado en metodologías probadas a nivel internacional.

- **Valoración de Seguridad Conforme a Estándares.**
- **Análisis y Tratamiento de Riesgo.**
 - Nivel de Procesos. Metodología BS7799 / ISO17799.
 - Nivel de Tecnología. Metodología OSSTMM.
- **Plan de Tratamiento de Riesgos.**
- **Clasificación de Información.**
- **Creación de Políticas de Seguridad.**
- **Cumplimiento a Normativa y Leyes.**
- **Programa de Concientización Organizacional.**
- **Diseño de Arquitectura de Seguridad.**
- **Diseño de controles de Seguridad.**

* **Nota:** es posible manejar como proyectos independientes cualquiera de estos temas.

SECURED SPECIALIST

NEXTIRADNE MÉXICO CUENTA CON UN GRUPO DE EXPERTOS CERTIFICADOS EN DIVERSAS ÁREAS DE LA SEGURIDAD EMPRESARIAL RESPALDADOS POR FABRICANTES Y ORGANISMOS DE SEGURIDAD.



Diseño de Sistemas de Seguridad en Redes Complejas.*

Basados en nuestra experiencia en la implementación de tecnologías emergentes y seguridad crearemos el mejor esquema que ayude a sostener la operación de su compañía.

- **Requerimiento previo:** Documento de Diseño de Sistemas de Administración de la Información.
- **Diseño de Sistemas de Seguridad en Redes Complejas que integre las soluciones dependiendo las necesidades específicas del cliente los elementos siguientes:**
 - Firewalls.
 - Sistemas de Detección / Prevención de Intrusos.
 - Sistemas de Correlación, Análisis y Respuesta de Eventos.
 - Sistemas de Control de Acceso en la Red.
 - Implantación de Seguridad para Soluciones de Telefonía IP.
 - Soluciones de Antivirus (Spyware, Spam, Malware, Virus) en Red y en Escritorio.

Definición de Políticas de Seguridad Organizacionales.*

Este servicio permite definir un conjunto de políticas de seguridad que incluyan tecnología, procesos y elemento humano a la medida de cada organización. Como por ejemplo:

- **Políticas de Uso de Encriptación en los Procesos.**
- **Políticas de Uso Aceptable de Recursos.**
- **Políticas de Asignación y Administración de Passwords.**
- **Políticas de Uso de E-mail y de Internet.**
- **Políticas de Atención de Incidencias de Seguridad.**
- **Políticas de Control de Acceso, etc.**

La definición de estas políticas permitirá al cliente contar un marco normativo sobre el cual se implantarán los controles tecnológicos en la organización.

* **Nota:** es posible manejar como proyectos independientes cualquiera de estos temas.

Elaboración de Plan de Concientización de Seguridad Organizacional.*

La creación e implantación de un plan de concientización organizacional propicia que todos los niveles de su empresa cuenten con el conocimiento adecuado de la importancia de la seguridad y sus repercusiones en el negocio.

Ayudando a reducir el intento de acciones no autorizadas, aumentar la efectividad de los controles de protección, evitar el fraude, desgaste y abuso de los recursos de cómputo y red.

La planeación del Programa de Entrenamiento y Conciencia de Seguridad considerará diversas formas de conciencia de seguridad que incluyan:

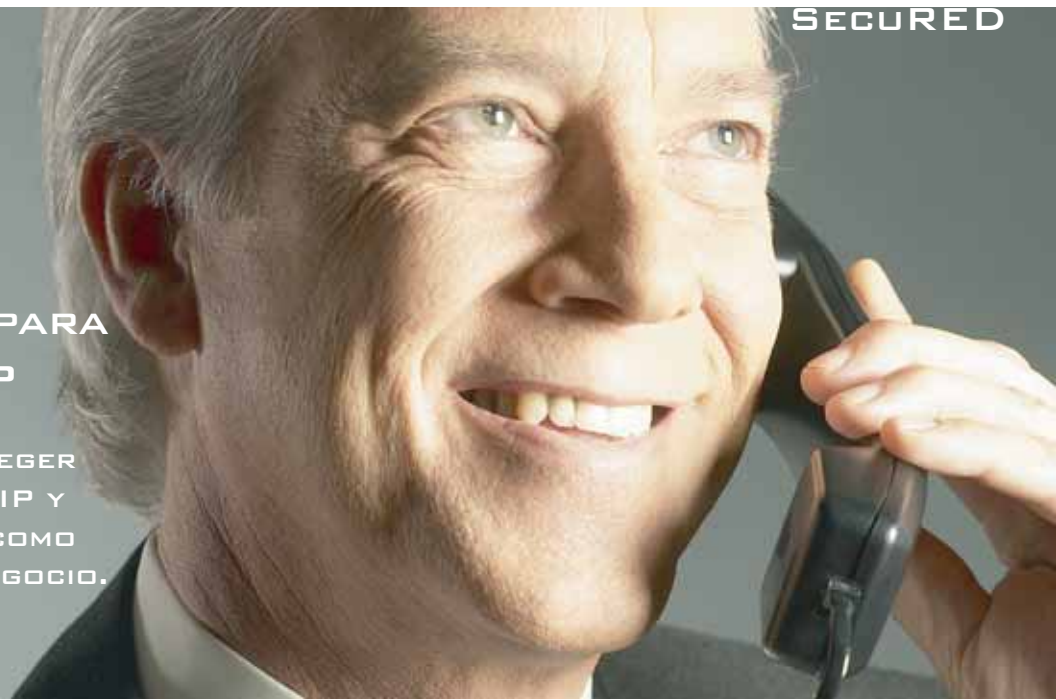
- **Elaboración de un programa de capacitación técnica y no técnica en diferentes niveles de la organización.**
- **Presentaciones interactivas en vivo. Demostración de pruebas de concepto, elaboración de presentaciones dinámicas y conferencias del tema de seguridad.**
- **Distribución de publicaciones. Carteles, periódicos, boletines e intranet.**
- **Incentivos. Premios y reconocimientos por logros en la seguridad.**
- **Recordatorios. Mensajes de recordatorio en elementos de oficina (plumas, mouse pads, stickers, etc.).**



* **Nota:** es posible manejar como proyectos independientes cualquiera de estos temas.

SEGURIDAD DE INFRAESTRUCTURA PARA COMUNICACIONES IP

ES UN SERVICIO DIRIGIDO
ESPECÍFICAMENTE PARA PROTEGER
SU INVERSIÓN EN TELEFONÍA IP Y
ASEGURAR SU CONTINUIDAD COMO
HERRAMIENTA CRÍTICA DEL NEGOCIO.



Seguridad de Infraestructura para Comunicaciones IP.

Una de las aplicaciones de misión crítica de las organizaciones son las comunicaciones de voz IP. Al ser los sistemas de telefonía IP una solución de datos, estos son tan seguros como la red misma que los soporta. Por tal razón, proveer seguridad a dicha infraestructura implica resolver la seguridad en múltiples capas que incluyen al menos:

Protección a la Infraestructura de Red.

El fortalecimiento de la infraestructura de red podrá incluir la configuración que mitigue y proteja de las siguientes amenazas:

- **Ataque de Overflow a las Tablas CAM de los Switches.**
- **DHCP Starvation.**
- **ARP Spoofing.**
- **VLAN Hopping.**
- **Manipulación del Protocolo Spanning-Tree.**

Asimismo, se incluyen recomendaciones de rediseño de la arquitectura misma con criterios de seguridad.

Protección a los Teléfonos y Sistemas de Control de Llamada.

La integración de tecnologías de encriptación mediante el uso de certificados digitales nos garantizan la autenticidad y codificación en las conversaciones y señalización de llamadas. Además es factible habilitar medidas de seguridad en los teléfonos como protección a ataques de ARP, protección a la VLAN de voz, etc.

Protección a las Aplicaciones.

Mediante la integración de la tecnología de IPS implementado en el servidor de Call Manager, obtenemos:

- **Protección de Intrusos Basado en Host.**
- **Protección a Ataques del Tipo Buffer Overflow.**
- **Protección de Gusanos de Red, incluso de Día Cero.**
- **Fortalecimiento del Sistema Operativo.**
- **Protección del Servidor Web.**
- **Seguridad para Aplicaciones del Servidor.**

Nuestra solución de implantación de seguridad la constituye la implementación multicapa de seguridad, visualizando todos los componentes como un sistema y no como piezas aisladas de tecnología.



www.NextiraOne.com.mx

MÉXICO

Av. Revolución 639
San Pedro de los Pinos 03800
México, D.F.
(55) 5010-7000

MONTERREY

Calz. del Valle 110 Ote. 1er. Piso
Col. del Valle 66250
Garza García, N.L.
(81) 1001-8000

GUADALAJARA

Av. Américas 161 P.B.
Col. Ladrón de Guevara 44600
Guadalajara, Jal.
(33) 3001-3000